

SCANNED

ATTACHMENT B

1. All records relating to violations of the statutes listed on the warrant in any form wherever they may be stored or found at 198 Concord Street in Portland, Maine, including:
 - a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;
 - b. records or information pertaining to an interest in child pornography;
 - c. records or information pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;
 - e. records or information pertaining to peer-to-peer file sharing;
 - f. photo editing software and records or information relating to photo editing software;
 - g. records or information relating to the occupancy or ownership of 198 Concord Street in Portland, Maine including, but not limited to, utility and telephone bills, mail envelopes, and correspondence.

2. Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including the receipt, possession, distribution, or transportation of child pornography in violation of Title 18, United States Code, Section 2252 and Title 18, United States Code, Section 2252A .

3. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment.
4. Records and things evidencing the use of the Internet, including:
- a. routers, modems, and network equipment used to connect computers to the Internet;
 - b. records of Internet Protocol addresses used;
 - c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).